DTIC FILE COPY

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

AD-A216 813

(2)

1a. REPORT SECURITY CLASSIFICATION	UNCLASSIFIED
1b. RESTRICTIVE MARKINGS	
2a. SECURITY CLASSIFICATION AUTHORITY	
2b. DECLASSIFICATION / DOWNGRADING SCHEDULE	
3. DISTRIBUTION / AVAILABILITY OF REPORT	Approved for public release; distribution unlimited.
4. PERFORMING ORGANIZATION REPORT NUMBER(S)	
5. MONITORING ORGANIZATION REPORT NUMBER(S)	AFOSR-TR- 89-1683
6a. NAME OF PERFORMING ORGANIZATION	CALIFORNIA INST. OF TECH.
6b. OFFICE SYMBOL (If applicable)	
7a. NAME OF MONITORING ORGANIZATION	Air Force Office of Scientific Research
6c. ADDRESS (City, State, and ZIP Code)	Department of Electrical Engineering Pasadena, CA 91125
7b. ADDRESS (City, State, and ZIP Code)	Building 410 Bolling AFB, DC 20332-6448
8a. NAME OF FUNDING / SPONSORING ORGANIZATION	AFOSR
8b. OFFICE SYMBOL (If applicable)	NM
9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER	AFOSR-83-0296
8c. ADDRESS (City, State, and ZIP Code)	Building 410 Bolling AFB, DC 20332-6448

10. SOURCE OF FUNDING NUMBERS

PROGRAM ELEMENT NO.	PROJECT NO.	TASK NO.	WORK UNIT ACCESSION NO.
61102F	2304	B1	

11. TITLE (Include Security Classification)

CODING FOR SPREAD-SPECTRUM CHANNELS IN THE PRESENCE OF JAMMING

12. PERSONAL AUTHOR(S)

Robert J. McEliece

13a. TYPE OF REPORT	13b. TIME COVERED	14. DATE OF REPORT (Year, Month, Day)	15. PAGE COUNT
FINAL	FROM 1 Jul 83 TO 30 Jun88		

16. SUPPLEMENTARY NOTATION

DTIC ELECTE JAN 16 1990 S D D

17. COSATI CODES

FIELD	GROUP	SUB-GROUP

18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)

19. ABSTRACT (Continue on reverse if necessary and identify by block number)

The research supported by this grant has led to a significantly improved mathematical understanding of the problems associated with communication in a hostile environment. The basic approach has been to apply the techniques and insights of information theory. The results obtained have given insight into how to best design communication systems which must function under severe noise. — RAH

20. DISTRIBUTION / AVAILABILITY OF ABSTRACT	☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT. ☐ DTIC USERS
21. ABSTRACT SECURITY CLASSIFICATION	UNCLASSIFIED
22a. NAME OF RESPONSIBLE INDIVIDUAL	DR NEAL GLASSMAN
22b. TELEPHONE (Include Area Code)	(202) 767-5026
22c. OFFICE SYMBOL	NM

DD Form 1473, JUN 86 Previous editions are obsolete. SECURITY CLASSIFICATION OF THIS PAGE

UNCLASSIFIED

90 01 11 129

Final Technical Report, 1 July 1983-30 June 1988

CODING FOR SPREAD-SPECTRUM CHANNELS IN THE PRESENCE OF JAMMING

(Grant No. AFOSR-83-0296)

Robert J. McEliece
Department of Electrical Engineering
California Institute of Technology
Pasadena, California 91125

Abstract: AFOSR.TR. 89-1899

The long-term goal of this project has been to obtain a basic mathematical understanding of the problems associated with communications in the presence of severe noise, e.g. jamming or fading. Our basic approach has always been to apply the techniques and insights of *information theory* to these problems. In our earliest work in this area, which was devoted solely to the jamming problem, we combined information theory with *game theory,* and obtained many insights about optimal jamming and antijamming strategies for a variety of realistic scenarios (Refs. [1]-[6]). Later, we studied more general models for severe noise (Refs. [7]-[13], and obtained results which we feel shed considerable light on how best to design communication systems which must function realiably in hostile environments.

Details:

In References [1]-[6], we studied many specific spread-spectrum modulation techniques, our goal being to identify the corresponding "worst case" jamming strategy. In some cases, our results have confirmed the conclusions of other researchers (e.g., in Ref. [2] we gave a rigorous proof of a result first announced by Houston about the worst-case jammer vs. a classical frequency-hopped system), but in many others, our results have been entirely new. We believe our most important results have been our development of an entirely new kind of "anti-jam" strategy involving the *randomization* of certain of the transmitter parameters. This technique was originally described in [2], but its most promising variation appears in [4], and [6], where we introduced the notion of the *random ration-threshold (RRT)*.

The RRT is based on another recent development in the field, Viterbi's *ratio threshold* (RT), a robust A/J countermeasure which has attracted considerable interest in the military communications community. We discovered several possibile weaknesses in the RT technique which can be remedied by a certain kind of parameter randomization. In fact, we proved that the RRT is superior by several dB's to conventional RT vs. many different jamming thresholds.

In reference [7], we embarked on a new direction for this project, and began an abstract study of the problem of reliable communication in the presence of extreme and unpredictable fading. There, using a remakable recent idea of Posner (IEEE Trans. Communications, April 1983, pp. 509-517), we studied this problem using the techniques of *broadcast coding*. Broadcast coding, which was invented in 1972 by Cover, is a commumication strategy which is normally applied to situations in which one individual must transmit information simultaneously to two or more receivers over two or more noisy channels. Posner's idea was to apply these results to a single physical transmitter and receiver, for which the transmission conditions are unknown, and to treat the possible transmission conditions as several "virtual" channels, corresponding the possible noise conditions. In this way, when the channel conditions are favorable, a large volume of information can be transmitted (this corresponds to transmitting over one of the "good" broadcast channels), but when conditions are unfavorable, nevertheless it is still possible to transmit critical information reliably, albeit at a slower rate (this corresponds to transmitting over one of the "bad" broadcast channels). In our paper [7], we showed that for a Gaussian broadcast channel (the broadcast channel model most appropriate for deep space and satellite communication), that for low signal-to-noise ratios, the sophisticated broadcast coding strategies devised by Cover and other researchers may not be significantly superior to the much simpler class of "timesharing" strategies. Our student, Eric Majani, has since shown that this same result (broadcast coding is not markedly superior to timesharing) is also true for very noisy binary symmetric channels. Since timesharing is much easier to implement than broadcast coding, this is an important point to know.

We also discovered that a serious study of very noisy broadcast channels requires a thorough understanding of very noisy (ordinary) channels. And although there is some published research on this topic, we found nothing in the literature which is quite what we need. Therefore, in [8], we completed what we feel is the definitive study of very noisy discrete memoryless channels (DMC's). In [8], we defined a class of very noisy DMC's, where the noise is controlled by a single parameter $\varepsilon \geq 0$, which we call the abstract signal-to-noise ratio. We found that DMC's fall into two different categories, one for which the capacity is proportional to ε, and the other for which it is proportional to ε^2, for small values of the signal-to-noise ratio ε. We have developed algorithms for calculating the constant of proportionality, for both classes of channels. We feel that this paper is the definitive work on very noisy DMC's; in any case, it is just what we needed for our study of very noisy broadcast channels.

In a related study, we made an information-theoretic investigation of the problem of optimal data compression. In [9], we have solved an outstanding problem in this subject, and computed the worst-case behavior of a certain class of quantization algorithms. And while it is too early to say exactly what practical importance this result may eventually assume, it is a nice example of how research in one area (in this case, communication in the presence of severe fading) may lead to results in another (in this case, data compression).

In our final series of papers ([11]-[14]), we investigated the performance of coded telecommunications systems, specifically binary phase-shift-delayed systems in the presence of Gaustian noise, at low signal-to-noise ratios. This is important because without a reliable theory, it is necessary to resort to elaborate computer simulations in order to find the performance at low snr's. We have discovered a reasonably simple formula [12] for the low snr performance that involves the distance spectrum of the code, together with anotner family of parameters. Also, in [13] we have identified a simple parameter (the so-called dominant-root) associated with any convolutional code which appears to accurately predict its performance at low signal-to-signal ratios. Extensive computer simulation confirms our belief in the importance of the dominant root; We hope that further research will provide us with a rigorous proof of it.

In summary, the research supported by this grant has led to a significantly improved mathematical understanding of the problems associated with communication in a hostile environment. This research is closely related to what others in this area have done, but contains many unique features (e.g. applications of game theory; tractible models for very noisy channels; the dominant root of a convolutional code). We feel that our results can contribute to greatly enhanced U.S. Communication security.

References

(all except [1] acknowledge AFOSR support)

[1] R. J. McEliece, "Communication in the presence of jamming-an information theoretic approach," pp. 127-166, in *Secure Digital Communications,* G. Longo, Ed., CISM Courses and Lectures, no. 279, Springer-Verlag, 1983.

[2] R. J. McEliece, E. R. Rodemich, "A study of optimal abstract jamming strategies vs. noncoherent MFSK," Proc. MILCOM '83, pp. 1-6.

[3] J. M. Borden, D. M. Mason, and R. J. McEliece, "Some information theoretic saddlepoints," SIAM J. Optimization, 23 (1985), pp. 129-143.

[4] L.-F. Chang and R. J. McEliece, "A study of Viterbi's ratio-threshold AJ technique," Proc. MILCOM '84, pp. 182-186.

[5] R. J. McEliece and W. E. Stark, "On the capacity of channels with block memory," IEEE Trans. Inform. Theory, 1988, Vol. IT-34, pp. 322-324.

[6] L.-F. Chang, *An information-theoretic study of ratio-threshold antijam techniques*, Ph.D. Thesis, University of Illinois, 1985.

[7] R.J. McEliece and L. Swanson, "A note on the wideband Gaussian broadcast channel," IEEE Trans. Communications, Vol. COM-35 (April 1987), pp. 452-453.

[8] E. Majani and R. J. McEliece, "A model for the study of very noisy channels and applications to binary input discrete memoryless channels," presented at 1988 International Symposium on Information Theory, Kobe, Japan. June, 1988.

[9] E. Majani, O. Collins, and Y. Abu-Mostafa, "Essential average mutual information," presented at the 1986 International Symposium on Information Theory, Ann Arbor, MI, October 1986.

[10] E. Mahani, *A model for the study of very noisy channels, and applications*, Ph.D. Thesis, California Institute of Technology, 1987.

[11] K. Abdel-Ghaffar and R. J. McEliece, "The ultimate limits of information density," Proc. 1986 NATO Advanced Study Institute on Performance Limits for Communication, Il Crocco, Italy, July 1986.

[12] R. J. McEliece, L. Swanson, and C. Chao, "The Behavior of Codes at Very Low Signal-to-Noise Ratios," presented at the 1988 International Symposium on Information Theory, Kobe, Japan, June 1988.

[13] C. C. Chao and R. J. McEliece, "Average Distance Structures of Random Convolutional Codes," Proceedings of the 1988 Allerton Conference on Communication, Control, and Computing, in press.

[14] C. C. Chao, *Behavior of Codes at Low Signal-to-Noise Ratios,* Ph.D. Thesis, California Institute of Technology, 1988.